Health Providers' Disaster Preparedness and Response: A Proposed Model for an Information Technology Solution

May 2003

John Leifer
Michael A. Grasso, PhD
Alyse Freilich

PREPARED FOR:
National Preparedness and Response Task Force,
Health Information and Management Systems Society
Chair: Colonel Rosemary Nelson

Introduction

The ability of the United States' healthcare system to respond effectively to large-scale disasters and emergencies rests on the quality and timeliness of the information available to healthcare providers and the communication between these providers and other critical constituencies. Not only do providers require specific data in order to contribute to deterrence and surveillance of public health threats, but also they need quickly- and easily-accessible, actionable information in order to participate most effectively in the response and recovery.

While the United States has made great strides in developing mechanisms to survey public health and protocols for response to specific threats, the fragmentation of the healthcare system continues to represent a significant barrier to our ability to ensure timely communication of accurate and appropriate information. Surveillance of the population to detect threats becomes extremely difficult without a means of aggregating the intelligence of each healthcare provider, and a coordinated response to a specific threat is impeded by the piecemeal nature of the system. Composed of a wide variety of organizations and facilities that have divergent needs and goals, the healthcare system is only loosely unified by local and state health departments and federal agencies such as the Centers for Disease Control (CDC).

The ability of emergency departments, hospitals, clinics, physician offices, first responders, laboratories, pharmacists, and school nurses to communicate with each other quickly may have enormous implications for the care of individual patients when the healthcare system is faced with a local, state, or national threat to public health. In the event of a bioterrorist event, for example, an attack may go unnoticed because of the lack of attention to early evidence. Increases in purchases of over-the-counter medications at grocery stores and drugstores, spikes in school or work absenteeism, and heightened complaints of seemingly common symptoms at primary care physician offices may fail to be detected independently, and the confluence of these factors, offering even greater evidence of a potential problem, would not be apparent. Furthermore, response to this event would strain the resources of a healthcare system that can estimate capacity only on a facility-level basis. The health department would be required to model resource needs and contact each healthcare organization in the affected region to determine availability of key personnel, beds, equipment, and supplies. Without instructions to the contrary, first responders would transport patients based on routine procedures, resulting in a potential breach of containment and misallocation of patients that, in turn, may result in a lethal lag time before treatment. Finally, the ability to monitor the spread of the disease would depend on constant telephone communication, and the difficulty inherent in ongoing surveillance during times of stress on the system would mean that additional threats or similar events in other localities may go undetected.

Current technological initiatives

While the advancement and proliferation of technology has significantly magnified the terrorist threat we face, it is also this very technology that can arm us with potent tools to respond to disasters and emergencies, both man-made and natural. Unfortunately, use of technology within individual hospitals and clinics lags other industries, and technology that facilitates communication and coordination between healthcare entities also remains underdeveloped. Numerous efforts to create and implement these systems are underway, however, and many of these systems may have important applications to the surveillance of and response to public health emergencies.

The need for a centralized information system that serves both federal and state agencies has never been more urgent. Inspired by the terrorist attacks of September 11, 2001, the anthrax deaths, and the SARS outbreak, federal and state governments, as well as private companies, have recently implemented a number of initiatives to create coordinated systems for surveillance, detection, and response. Indeed, in the last several years, a substantial number of new systems have been created and, in some cases, implemented, resulting in a wide variety of options for both providers and governments seeking solutions to the data collection, analysis, and communication challenges they face. An Agency for Healthcare Research and Quality (AHRQ) report on information technology for bioterrorism preparedness and response found 217 existing information technology/decision support systems (IT/DSSs) of potential use in the event of a bioterrorist attack or other public health emergency, most of which were developed for detecting naturally occurring illnesses.[1]

More importantly, these off-the-shelf systems developed by private companies are joined by a number of initiatives at the federal and state government levels. The CDC has now collected its bioterrorism preparedness efforts under the umbrella concept of the Public Health Information Network (PHIN), an architecture for a standards-based network of systems. PHIN seeks to create an interoperable network that offers a common framework of standards and specifications for integrating public health systems and functions while using industry information technology standards. This unified network offers standards for detection and monitoring, analysis, knowledge management, communications, and response capabilities. PHIN builds on existing federal initiatives such as the Health Alert Network (HAN) and the National Electronic Disease Surveillance System (NEDSS), as well as other efforts to collect national data on public health for detection purposes. Other federal initiatives include the National Health Information Infrastructure (NHII), new communication systems to alert physicians nationally to an identified public health crisis, and BioSense, a system to enhance the nation's ability to access and analyze health data for bioterrorism indicators.

[1] Agency for Healthcare Research and Quality, "Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems," June 2002.

At the state level, there also appears to be a wide variety of systems conceptualized or implemented. The increase in the availability of federal dollars for states, coupled with the increased threat of disease, has spurred substantial activity in this area. The Department of Health and Human Services appropriated $1.1 billion for bioterrorism during fiscal year 2002, with $918 million going to states through the CDC and another $125 million distributed to hospitals through the Health Resources Services Administation. Example programs include Pennsylvania's Real-time Outbreak and Disease Surveillance (RODS) program, a public health surveillance system, and California's initiative to develop a Rapid Health Electronic Alert, Communication, and Training (RHEACT) system.

Despite this increase in the number of preparedness efforts underway, it appears that the vast majority of these systems focus almost entirely on surveillance and do not address the need for communication with providers and for modeling activities during the response to an event. Furthermore, the lack of coordination and standards among these initiatives not only result in duplicative efforts and inflated costs, but also they preclude the ability to create a nationally integrated system that would allow the federal government to observe national patterns and trends. Aware of this lack of coordination and standards, members of Congress are currently debating the creation of a national disease reporting system, as well as enforcement of uniform standards for disease reporting. A key question, at this point, is whether there will be a national system with one data warehouse, centralized surveillance by the federal government, and threat identification and coordination responsibilities on a national level, or if these efforts will be designed and directed at the state level, with bi-directional communication with federal agencies.

Objectives

In this white paper, we present a starting point for discussion of this question by suggesting roles for the federal and state governments and by taking initiatives currently in place one step further. We build on the work done by the CDC and others to conceptualize (at a high-level) the construction of a nationally deployed health information infrastructure that would support optimal and timely provider surveillance as well as response. We identify the responsibilities of the federal and state governments in this proposed system, the functions required by the system, and the technological standards that would ensure its success. There are, of course, many different approaches to this very complex problem; this paper is intended simply to present one model for solution and to provoke the national dialogue necessary for consensus to be achieved.

While this paper was developed for members of the Healthcare Information and Management Systems Society (HIMSS), it is intended for a wide range of audiences, including (but not limited to) the defense and intelligence communities, state and federal officials involved in preparedness efforts, and health care providers throughout the country who are interested in the creation of a responsive information network to address potentially catastrophic events. Please note that while the focus of this paper is on bio-events (bioterrorism and natural diseases), the infrastructure we present is equally

applicable and critical to supporting a response to chemical, nuclear, and natural disasters. Furthermore, although the infrastructure we propose may serve as the source of information for all organizations involved in these events (e.g., law enforcement, Homeland Security, etc.), we focus here on health providers' role in creating and utilizing this information.

Conceptual overview of surveillance and response system

We present a decentralized model for a comprehensive information technology infrastructure, giving states responsibility for collecting and disseminating all necessary information and coordinating surveillance and response. State-developed systems, however, must be compatible with each other and with federal systems, enabling the federal government to oversee a national network. In addition to collecting and analyzing a plethora of detailed data that facilitate threat identification, state governments are responsible for managing an emergency at a micro-level, determining necessary resources and capacity at local health facilities and directing patients to specific institutions. The federal government simultaneously accesses summary data from each state, consolidates data from all states, and analyzes this national data warehouse to discern national patterns and trends. Most states have already begun work in this area, and the envisioned system offers each state the flexibility to continue to design and implement a surveillance and response system that best meets its needs, as long as the state includes certain key functions and common technological standards that allow for federal consolidation. As shown in Chart 1, each state's system must include the components listed below.

- *State data warehouse.* Each state must create a centralized state data warehouse that contains aggregated health information, standardized protocols, and inventories of available resources. The data warehouse resulting from this collection ensures that all constituencies have immediate access to standards and protocols, that there is a baseline against which incoming data can be continuously compared, and that resources can be quickly assessed and distributed.

- *Decision Support and Alert System.* States will implement a decision support and alert system (DSAS) that mines the data warehouse for evidence of potential bio-events, facilitates simple and fast communication between all constituencies involved, and uses information contained in the data warehouse to model the scope of the threat and the resources needed for treatment and containment. As mentioned earlier, many private companies have developed off-the-shelf products that serve this function, and states are free to select any that meets the technological standards established.

- *State Coordinating Entity.* Each state must designate a State Coordinating Entity to oversee surveillance and to coordinate activities during an event. It is anticipated that the Coordinating Entity will have a human analysis process in addition to computer analysis, ensuring that epidemiological expertise verifies computer-generated alerts and allowing for human critique of computer-generated modeling. The State Coordinating Entity will most likely be part of the State Health Department or the

State Department of Homeland Security. Regardless, this entity will ensure close communication with state and local health departments.

State surveillance and response system functionality

With the data collection, monitoring and analysis, communication, and modeling capabilities described above, each state will have the critical abilities to deter potential threats, survey the population to detect threats, respond to a county, state, or regional emergency with treatment and containment, and recover from these events. We delineate the specific functionality required of the state systems in each of these phases below.

- **Deterrence**: While deterrence activities are primarily the domain of law enforcement and intelligence, healthcare providers may contribute to deterrence of both naturally-occurring diseases and bioterrorist threats through vaccination. Vaccination, it must be noted, may have limited value, as there are significant risks associated with mass vaccinations, the efficacy of vaccines against genetically modified or novel pathogens is uncertain, and mass vaccination against all potential agents is impossible. As vaccination is, however, currently endorsed by the federal government, the system we envision facilitates this process, ensuring that the provider community is aware of the need to vaccinate for specific diseases, understands specific protocols for vaccination, communicates vaccinations performed to other constituencies, and monitors reactions to vaccinations. The CDC and state health departments enter vaccination requirements and protocols into the various statewide data warehouse, and providers use a DSAS to access this information. All vaccinations performed are entered into the data warehouses, and each DSAS monitors reactions of vaccinated individuals who return to providers for treatment.

- **Surveillance**: In order to monitor the population for potential disease outbreaks, each state's system must educate constituencies, collect cumulative data on an ongoing basis, compare these data to baseline data, and evaluate specific alerts. Not only does the system analyze cumulative data on a continuous basis to detect significant deviance from baseline norms, but also it uses protocol-based alerts to identify specific cases that appear suspicious. Chart 2 presents the flow of information and the interaction between healthcare providers and other constituencies during this phase.

    - *Education.* The CDC, as well as other federal and state agencies, submit information concerning disease symptoms and treatment protocols to the state data warehouses. Providers are able to access this information to ensure that they will be able to recognize (and diagnose) suspicious cases.

    - *Data collection and analysis.* Incorporating and building on surveillance systems currently in existence throughout the United States, each state's system would receive data electronically from a broad array of agreed-upon sources that may include but would not be limited to the following: electronic medical records, core disease reporting, 911 calls, laboratories,

bio-sensors, over-the-counter drug retailers, and veterinary and agricultural data sources. Automated filter processes would clean these electronic data before they enter the data warehouse to ensure the validity of the information. Providers may also submit data manually using web-based data input screens, allowing physicians in small offices and school nurses to contribute to the cumulative data and forming a "civilian biodefense network."[2] Finally, providers who believe they have identified a patient with an infectious disease may submit information concerning the case and flag it for immediate review. A DSAS would use these data to create a set of baseline data and to monitor incoming data for any statistically significant variations. It should be noted that this system supplements many existing surveillance activities and does not necessarily replace them.

- *Protocol-based alerts.* A DSAS, using standardized diagnostic protocols, alerts providers when they enter symptoms that may be indicative of specific diseases. In addition, the system continually analyzes data in the comprehensive data warehouse and sends alerts to the Coordinating Entity when pre-determined conditions (for cumulative data or individual cases) are met.

- *Evaluation*. Epidemiologists (Analysis) evaluate protocol-driven threat notifications, using their expertise to offer further analysis of computer-based alerts and ensuring that computer errors do not result in unnecessary concern or action.

- **Response**: In the event of a disaster, the state Coordinating Entity, in conjunction with healthcare providers, will be responsible for coordinating the necessary resources (personnel, equipment, and supplies), clearing appropriate space and facilities to care for patients (and quarantine if necessary), triaging cases, and treating patients. At the same time, they would need to survey the population for new cases and communicate their efforts/progress to other constituencies and the media. In order to facilitate these activities, the communications, analysis, and modeling capabilities in the proposed system would enable the following steps, as shown in Chart 3:

  - *Initial alert.* After identifying a threat (either from the state system or the federal government), the system would allow the Coordinating Entity to alert all federal and state agencies, suppliers, and providers to the event. Using contact information stored in the database, the Coordinating Entity would be able to select organizations to be notified quickly and would be able to communicate the nature of the event and any other relevant information in the first moments after detection. There must be strict

[2] Ronald E. LaPorte, Francois Sauer, Steve Dearwater, Akira Sekikawa, Eun Ryoung Sa, Deborah Aaron, and Eugene Shubnikov, "Towards an Internet Civil Defence Against Bioterrorism," *The Lancet*, September 2001.

protocols for this communication, however, to ensure that the information is distributed securely only to appropriate individuals; inappropriate disclosure could result in mass panic that would impede effective response.

- *Requests for capacity assessment*. In addition to alerting providers to the event, the Coordinating Entity would request capacity assessment from each provider, both current and forecast for the next 48 hours, in eight hour increments. Resources to be assessed (personnel, beds, supplies, pharmaceuticals, and equipment) would vary depending upon the specific emergency. The Coordinating Entity would send a similar request to pharmaceutical, supply, and equipment (both standard and specialized) suppliers.

- *Model severity and spread* of event. The system's modeling capabilities would allow the Coordinating Entity to estimate severity and spread and to determine resources necessary for treatment and containment. The CDC's current capabilities to meet this need would ideally be incorporated into each state's system.

- *Capacity responses.* In events that result in mass casualties, there may be an immediate need for a large number of beds. The Department of Health and Human Services has suggested that regions be prepared to accommodate a sudden surge of 500 acutely ill patients, and many experts believe this number to be a substantial underestimate. Providers would determine their maximum potential capacity over the next 48 hours, in eight hour increments and by bed type: adult, critical care, pediatrics, nursery, emergency department, and other available beds. They would also identify the number of patients who, based upon established protocols, would be low-risk candidates for immediate discharge and those who could be expected to be discharged over the next 48 hours, in eight-hour increments. Providers and suppliers would then use the system to submit their potential capacity assessments to the data warehouse.

- *Allocation plan*. The Coordinating Entity uses the modeling capability within the DSAS to aggregate provider and supplier capacity information and compare these data to the resources necessary. The DSAS models an allocation plan, and the Coordinating Entity evaluates and finalizes this plan. This plan would include numbers of low-risk patients to be discharged at various facilities, the distribution of patients (of varying levels of treatment need) to particular providers within the region, and the allocation of supplies and equipment to be sent to providers.

- *Allocation plan dissemination.* The Coordinating Entity uses the system to communicate the allocation plan to providers, first responders, and suppliers.

- *Inventory activation.* After receiving the allocation plan, providers will clear beds, prepare the facility to receive patients, and use the DSAS to alert necessary staff. Similarly, suppliers send supplies allocated to appropriate facilities.

- *Treatment protocols.* Providers access treatment protocols for specific emergencies through the system. While these protocols currently exist, housing them within a centralized data warehouse ensures that any revisions to these protocols are immediately available to all providers.

- *Monitoring and allocation plan revision.* Ongoing provider input into the data warehouse ensures that the Coordinating Entity is abreast of the spread of the disease, the severity of the illness, and the progress of patients being treated. The Coordinating Entity uses this information to update its models for the spread of the disease and the resources needed for treatment and containment.

- *Continued surveillance.* During the response to a particular event, the envisioned system ensures ongoing surveillance for similar incidents in other areas or new threats.

- **Recovery**: After the population has been treated and the event has been successfully contained, the technology solution facilitates ongoing surveillance, mental health coordination, inventory restocking, and strategic planning for future events.

    - *Surveillance.* The system continues to monitor public health, with a specific focus on those recently treated and on recurring symptoms of the outbreak.

    - *Coordination of mental health resources*. As with the response allocation plan, mental health providers submit their capacity information, and the Coordinating Entity uses the DSAS to create an allocation plan that offers adequate grief and trauma counseling.

    - *Restocking inventory.* The system uses data collected concerning inventory (of vaccines, supplies, etc.) at each facility, determines quantities needed, and requests that inventory be moved from suppliers to providers where necessary. This effort ensures that all facilities are returned to pre-event status.

    - *Strategic planning:* The system creates retrospective, time-stamped reports, enabling evaluation of the response and strategic planning for future events.

Technological standards

In addition to creating systems that are capable of performing the functions delineated above, states must ensure that certain technical standards are in place so that the warehouses are interoperable and the federal government may access and aggregate state data warehouses to create a national network. We outline here the standardized language, data model, and security standards we believe are necessary to allow all data warehouses in the system, both state and federal, to communicate easily with each other and share key data needed at all levels of the process.

In order for the systems to communicate with each other they must use a common language. HL-7 has been the industry standard, but it should include the vocabulary fields LOINC® (Logical Observation Identifiers Names and Codes) and the Systematized Nomenclature of Medicine – Clinical Terms, better known as SNOMED-CT®, for the pooling of lab and other clinical results. Additionally, all monitoring and surveillance systems used at the state level should be compatible with standards identified in the CDC's Public Health Information Network (PHIN).

There should also be a standardized data model based on HL7-RIM (Reference Information Model) similar to the Public Health Logical Data Model (PHLDM), and data transport –"Handshake Between Information Systems" – should be standardized to ebXML (Electronic Business using eXtensible Markup Language). These specifications enable enterprises of any size and in any geographical location to conduct business over the Internet.

Finally, in order to ensure that communications are secure we suggest using a PKI (Public Key Infrastructure) approach. The National Institute of Standards and Technology (NIST) is currently leading the development of a Federal Public Key Infrastructure that would support digital signatures and other public key-enabled security services. The implications of the Health Insurance Portability and Accountability Act (HIPAA) for the aggregation and mining of data must also be taken into account.

Conclusion

This paper provides a starting point for the aggressive discussion and debate necessary to achieve a shared vision for addressing this complex problem. The model we present outlines, at a high level, the functionality necessary for states to conduct not only deterrence and surveillance, but also response and recovery most efficiently and successfully. While the model offers each state a certain amount of latitude in its approach to achieving this functionality, it also establishes the need for standards for language, data model, and communications protocols that are key to the success of a nationally integrated system.

There are today a vast and ever-increasing number of technology options available to all constituencies involved in bioterrorism preparedness. Indeed, new initiatives are introduced each day to solve specific segments of this problem, and the need for a

national system as soon as possible drives continuing efforts in both the public and private sectors. The support and participation of all providers is necessary for the creation of an effective system, however, and the significant costs that face providers, states, and the federal government remain a primary barrier to achieving this support.

As health care providers observe the discussions and changes occurring at the national and state levels and begin to consider their roles in a national preparedness system, they must be aware of the requirements such a system imposes on their organizations and they must proactively establish a voice for themselves in these discussions. First, an understanding of the required data formats and communication protocols required by state Coordinating Entities for data collection activities will inform the way in which providers choose to collect their data and the information technology purchases they make. In addition, providers must be aware of the data offered by the CDC and the state Coordinating Entity and the means of accessing these data. Finally, providers must be familiar with appropriate communication mechanisms with the state Coordinating Entity, from alerting authorities to potential emergencies to communicating capacity information.

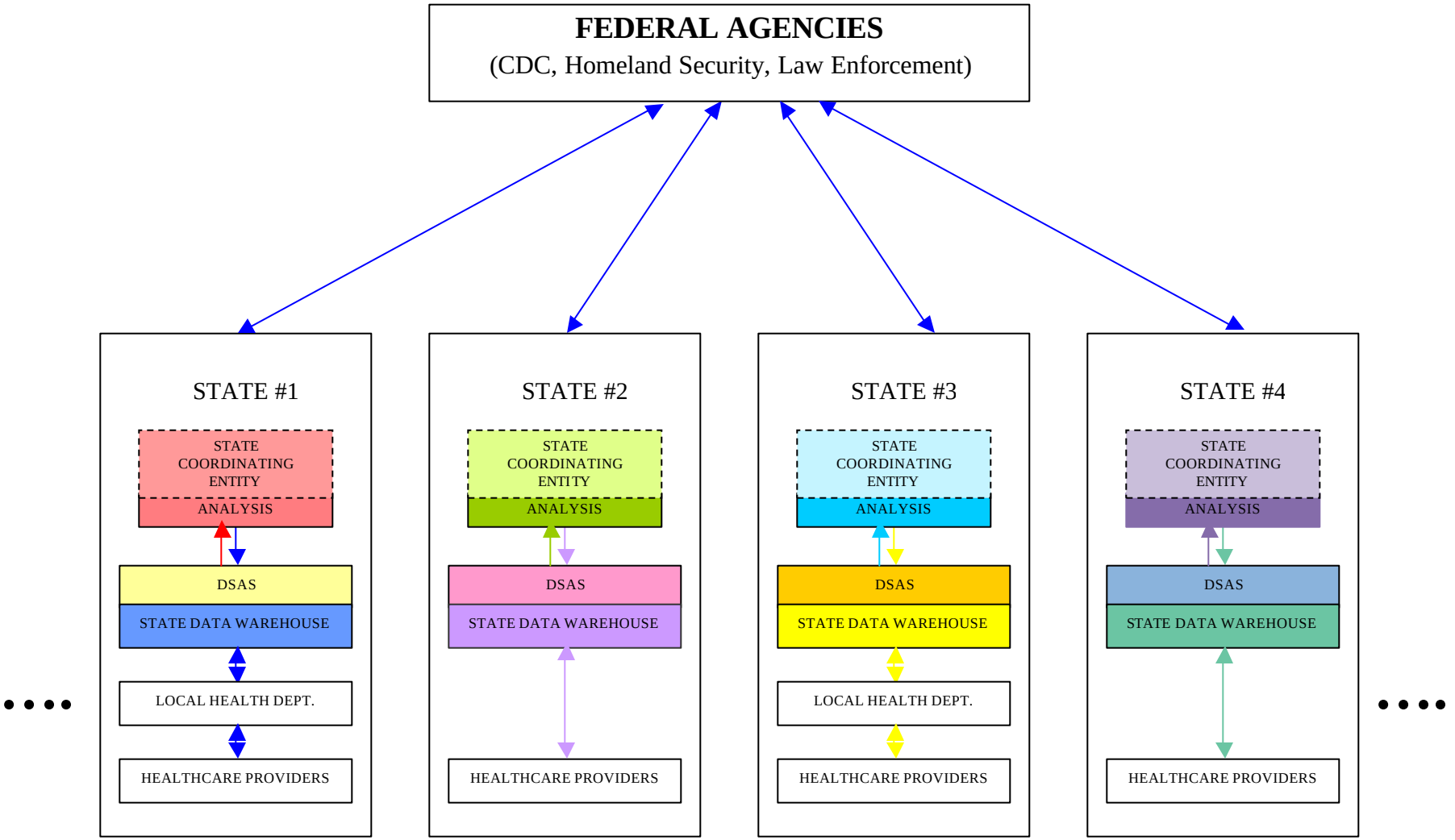
As the United States moves forward in this arena, there is much work yet to be done before the benefits identified in this conceptual model may be realized. Before addressing the challenge of implementing such a system, substantial research efforts are necessary to build detail into the model. A comprehensive survey of the activities and developments within each state, for example, would define the immediate capabilities of our surveillance and response systems and allow for knowledge sharing between states and others involved in this challenge. Furthermore, this survey would result in an assessment of the current standardization that exists and would lead to further research efforts concerning detailed technological standards and the cost of compliance with common standards.

Whether technology becomes an enabler of powerful new threats or a potent tool in improving the security of our health system and the safety of our population is wholly contingent upon the development of a shared vision for an information technology solution. The race to create solutions at every level of the public and private sectors testifies to the great need and enormity of the problem, but we run the risk of developing disparate models that cannot be unified into a national network and spending resources needlessly on duplicative efforts. Consensus around a guiding vision is critical to our ability to move forward efficiently and to create a system that meets the needs of all constituencies involved.

Acknowledgements

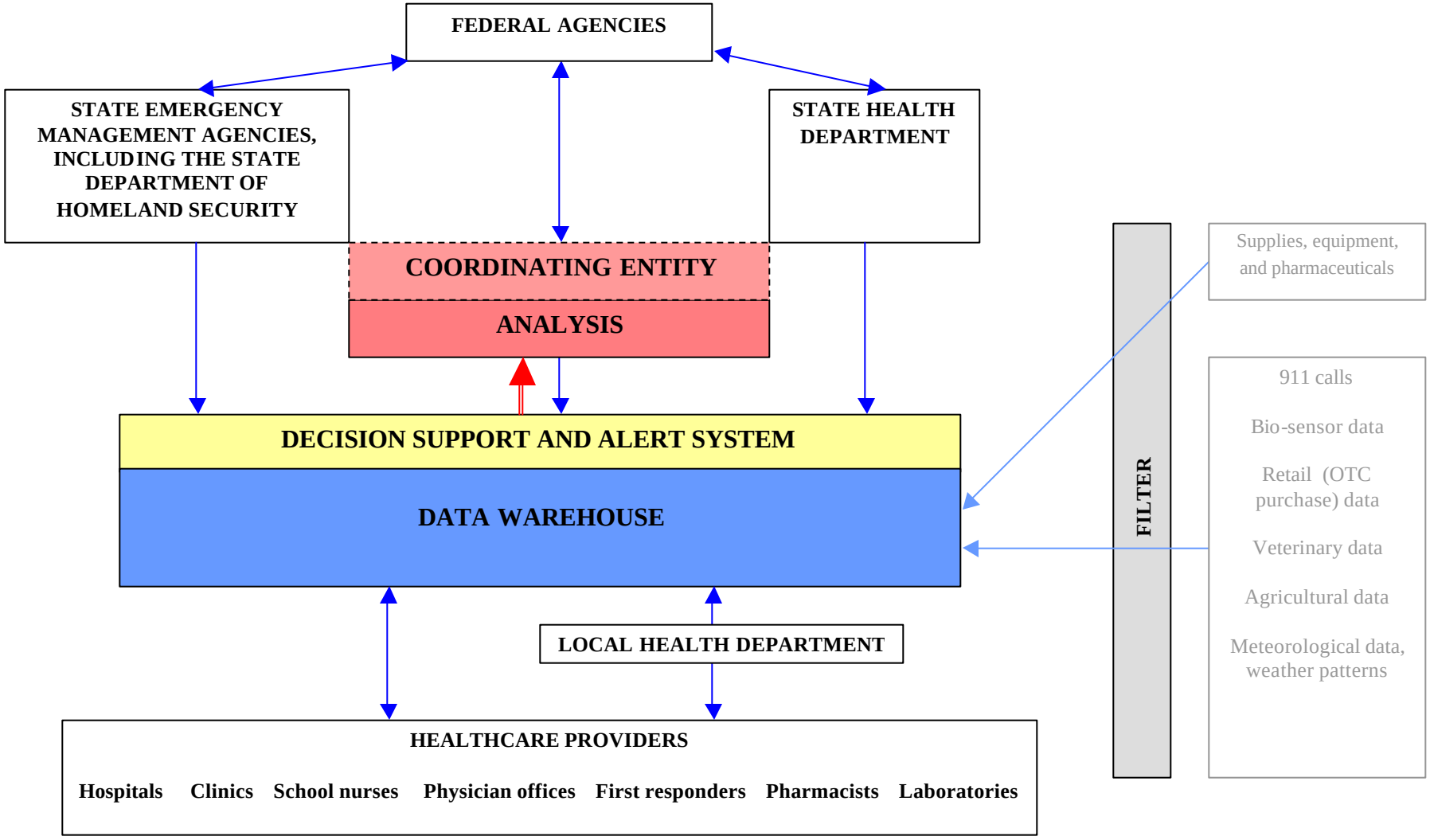
This report was prepared for the National Preparedness and Response (NPR) Task Force of the Health Information and Management Systems Society (HIMSS). Several task force members and subject matter experts made important contributions to the content of this paper, including John Loonsk, M.D., CDC; Richard Hopkins, M.D., CDC; Jim Flannigan, M.D., Language and Computing Inc.; William Davenhall, ESRI; Jonathan Schaeffer, M.D., Cleveland Clinic Foundation; Linda Reeder, R.N., Envision Consulting; and Rick Curtis, MIKON Systems. Colonel Rosemary Nelson, the chair of the NPR Task Force, and Carla Smith at HIMSS also provided helpful comments on draft versions of this report. The opinions expressed in this report and any errors or omissions, however, should be interpreted as those of the authors.

Chart 1. Standard Functions, Variable Approaches



While each state will have the required functions of Coordinating Entity, Analysis, DSAS, and Data Warehouse, there may be variation among states' development of these functions. There should, however, be agreement on standard language (HL-7) and communication protocols (ebXML).

Chart 2. State Surveillance Model

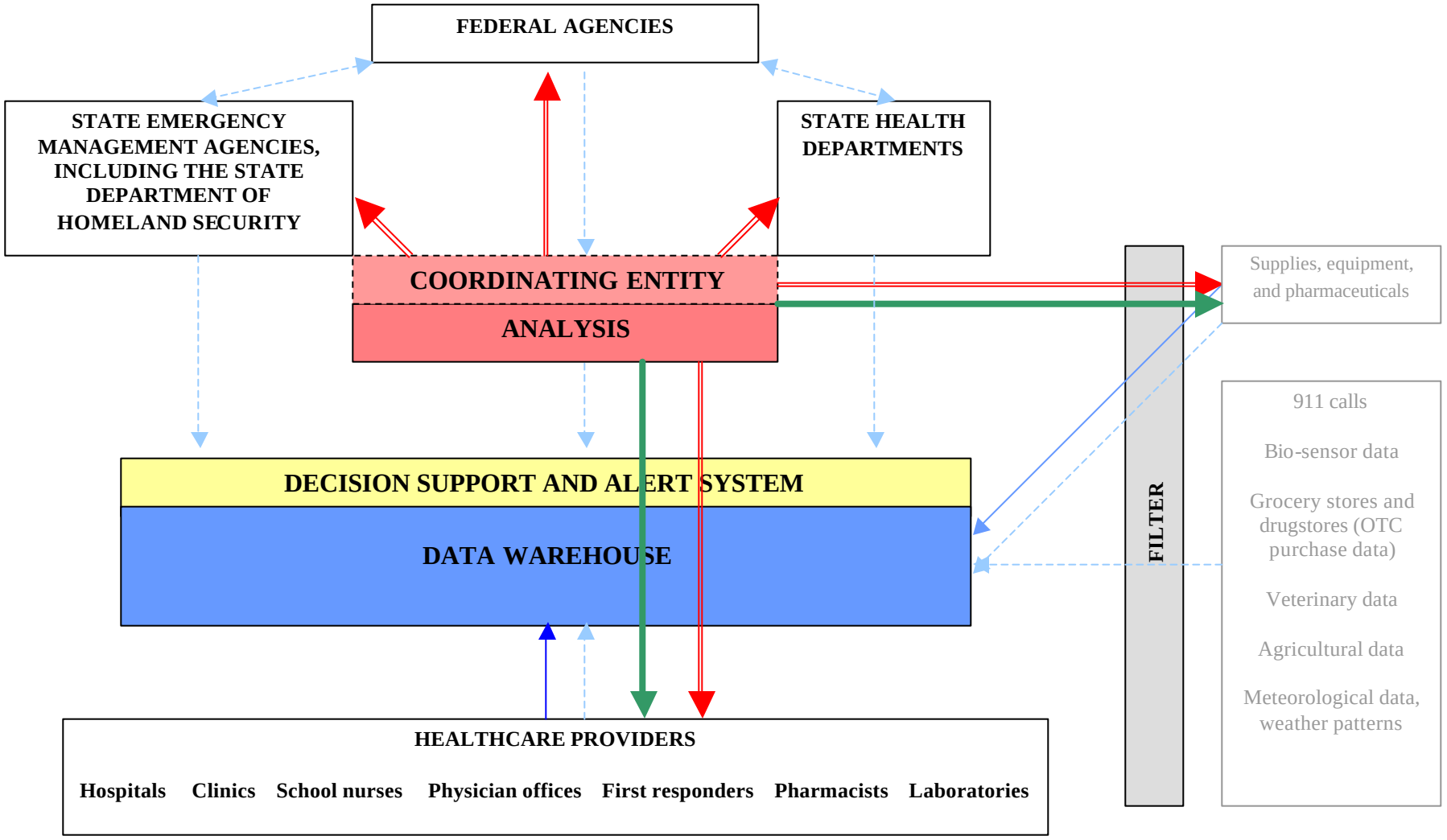


- Providers and others **submit** cumulative diagnostic and symptom data, information concerning suspicious cases, vaccinations performed, laboratory results, and information concerning resources available.
- Providers **receive** reminders, learn about infectious disease symptoms, and educate themselves concerning protocols.
- CDC and state agencies submit vaccination information and protocols, resources required for specific disasters, transmissibility, treatment protocols, community demographics, etc.

Protocol-driven Decision Support System aggregates data and automatically issues alerts to Analysis.

Analysis evaluates and verifies alerts from Decision Support System.

Chart 3. State Response Model



- Analysis issues alerts for real threats.
- Analysis requests capacity information from providers & suppliers
- Analysis models scope of threat and capacity requirements

Providers and suppliers submit capacity availability to data warehouse

Decision support system aggregates capacity availability and creates recommended allocation plan.

Analysis validates DSS"s recommended allocation plan and communicates it to all providers and suppliers.

Surveillance activities (described on previous chart) continue, in an effort to monitor spread of disaster or new threats.

